SPOOFING REPORT

ABSTRACT

While drones continue playing a vital role in a large number of industries, securing communication systems for these drones against attacks such as ADS-B (Automatic Dependent Surveillance–Broadcast) spoofing is of utmost priority. This paper considers the drawback of a naive ADS-B spoofing attack and introduces a new solution in which it employs gradual spoofing for realism and stealth. The first realization of this attack comprised sudden, large alterations in position data of a drone, which rendered it highly detectible using anomaly detection systems. The new solution, however, employs minute, sequential alterations in latitude, longitude, and height over time, which is highly similar in actual-world GPS spoofing strategies. This process of gradual spoofing makes it highly challenging for detectability, which makes it highly suitable for security testing and evaluation. Through enhanced spoofing strategies, this paper contributes toward enhanced security studies in drones, which provide a highly realistic simulation of vulnerability in cyber-physical systems and guide in developing highly effective countermeasures for attacks based on GPS.

INTRODUCTION

With the expanding use of drones in numerous fields, it has also become vital that they be protected against cyber-attack, especially against spoofing of their communications system. One such spoofing attack involves ADS-B spoofing, wherein false position information is injected with the intention of deceiving the navigation system of the drone. This study investigates the effect of ADS-B spoofing and seeks to enhance attack simulation through the use of gradual spoofing techniques that better simulate real-world cyber-attack behavior. Compared with sudden position shifts, the gradual spoofing technique varies telemetry in small increments and becomes difficult to detect and also increases the effectiveness of the attack

TYPES OF SPOOFING

Spoofing attacks can take many forms and are often used in cyberattacks to gain unauthorized access, steal information, or spread malware. Awareness of these types of attacks is crucial for individuals and organizations to implement effective security measures and protect against potential threats. The following are some few spoofs mentioned;

A. IP Spoofing:

- It Involves sending IP packets from a false (or "spoofed") source address to disguise the sender's identity. This technique is often used in denial-of-service attacks.

B. GPS Spoofing

- Involves sending false GPS signals to mislead a GPS receiver about its actual location. This can be used to manipulate navigation systems or location-based services. This drone simulation mostly deals with the GPS spoofing

C. Caller ID Spoofing:

- This spoof alters the caller ID information transmitted to the recipient's phone, making it appear as though the call is coming from a different number. This is often used in scams and telemarketing.

D. Wi-Fi Spoofing (Evil Twin Attack)

- Attackers set up a rogue Wi-Fi access point that mimics a legitimate one, tricking users into connecting to it. This allows attackers to intercept data transmitted over the network.

The other types of spoofing are; DNS spoofing (DNS cache poisoning), Address Resolution Protocol (ARP), Website spoof, Social Media Spoofing, Malware Spoofing, Session Hijacking, etc.

IMPLEMENTATION

The initial spoofing mechanism in the Drone-Sim project modifies drone telemetry data by applying random deviations to latitude, longitude, and altitude. The key features of this implementation include:

- **Abrupt Spoofing Changes:**
  - Latitude and longitude variations of ±0.05 degrees.
  - Altitude jumps of ±50 meters.
  - High detectability due to sudden positional shifts.
- **Limited Realism:**
  - Spoofed data does not simulate real-world attack patterns, which typically involve gradual drift to avoid detection.
- **Randomized Drone Identity Alteration:**
  - The original given code occasionally replaced the actual drone ID with a fake one, creating a simplistic spoofing effect.

After enhancements and modification of drone simulation the shortcomings of the original code implementation was shown. Below is an outline of the analysis of implementation modifiers that were denoted:

Feature	**Original Code**	**Modified Code**
Latitude & Longitude Drift	Random variation of ±0.05 degrees	Controlled variation of ±0.005 degrees
Altitude Drift	Abrupt changes of ±50 meters	Gradual drift of ±0.5 meters
Detection Risk	High due to sudden shifts	Low due to smooth transitions

Realism	Basic and unrealistic	Mimics real-world attack patterns

Table 1: Comparison between Original code and Modified code

RESULTS AND OBSERVATIONS

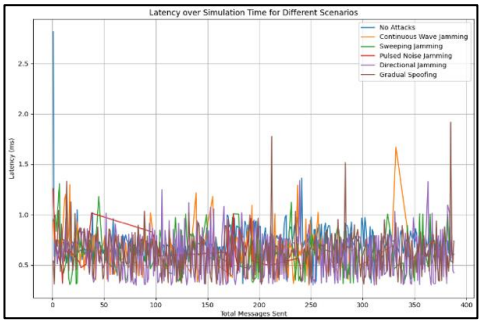

Fig 1: Latency Plot (latency_plot.png): Shows how different jamming techniques affect drone communication delays.

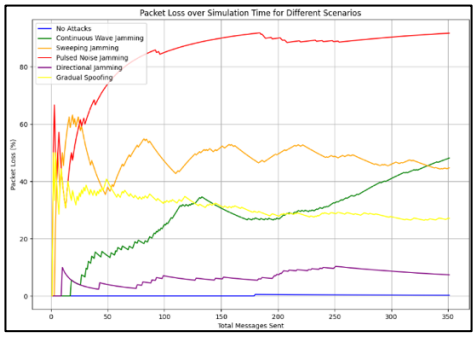

Fig 2: Packet Loss (packet_loss.png): Illustrates how much data transmission is lost under each jamming attack.

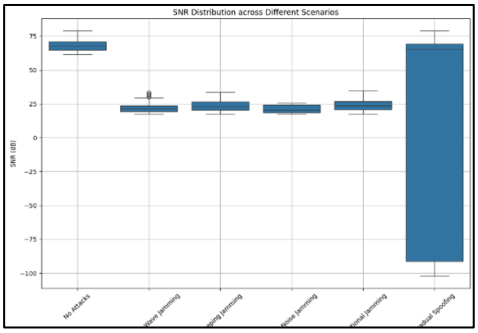

Fig 3: SNR Box Plot (snr_box_plot.png): Represents the signal-to-noise ratio variations caused by jamming.

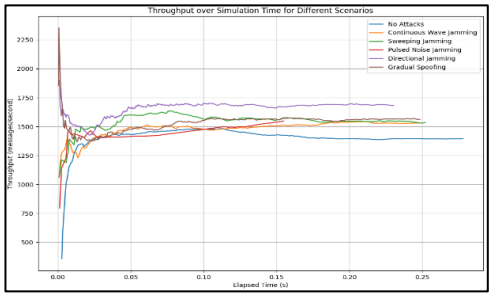

Fig 4: Throughput Plot (throughput_plot.png): Displays the impact on data transmission efficiency

- **Smooth Transition Mechanism:**
  - Instead of sudden jumps in position, the updated code modifies coordinates incrementally (±0.005 degrees for latitude/longitude, ±0.5 meters for altitude), creating a seamless drift effect.
- **Adaptive Spoofing:**
  - The new implementation introduces adaptive spoofing where the drift is applied progressively over time rather than in one abrupt change, reducing the likelihood of detection.
- **More Realistic Attack Simulation:**
  - The spoofing follows patterns closer to real-world GPS spoofing attacks, where attackers slowly manipulate navigation data to mislead the system without raising alarms.
- **Code Maintainability & Scalability:**
  - Well-defined variables for drift values allow easy adjustments to experiment with different spoofing intensities.

CONCLUSION

The updated code provides a significant improvement over the original ADS-B spoofing implementation. By introducing gradual drift in the drone's position data, it mimics real-world GPS spoofing attacks more effectively, making detection more challenging and enhancing the overall realism of the simulation. The gradual spoofing approach offers flexibility, realism, and better control over the spoofing attack, which are essential for simulating realistic cybersecurity threats to Cyber-Physical Systems (CPS), particularly in the context of drones. This enhanced model is a crucial step forward in testing and analyzing drone security vulnerabilities and provides a more effective platform for evaluating the consequences of GPS spoofing in both cyber and physical domains

REFERENCES

[1] Austin, R. (2010). *Unmanned aircraft systems: UAVs design, development and deployment*.

[2] Fahlstrom, P. G., & Gleason, T. J. (2012). *Introduction to UAV systems* (3rd ed.).

[3] *MITRE ATT&CK*. (2015). The MITRE Corporation. Retrieved February 26, 2025, from https://attack.mitre.org/

[4] Joshi, R. C., Jain, A. K., & Gupta, S. K. (Eds.). (2019). *Security and privacy in Internet of Things (IoT) and cyber-physical systems*. Springer.